GIFT-64 算法的 Biclique 分析

郭伟博[1]，刘 彬[1]，王 洋[2]

(1.信息工程大学，郑州 450001; 2. 西安测绘总站，西安 710054)

摘 要：GIFT 算法是一种实现效率高、所需功耗低的轻量级分组密码算法，现有评估其安全性的研究成果较少。、利用 Biclique 攻击方法，结合算法密钥调度方式以及轮函数结构的信息泄露规律，分别给出了对于 GIFT-64 算法的平衡 Biclique 攻击和 Star 攻击结果。对于 GIFT-64 算法的平衡 Biclique 攻击所需的数据复杂度和计算复杂度分别为 2^{32} 和 $2^{127.36}$；对于 GIFT-64 算法的 Star 攻击所需的数据复杂度和计算复杂度分别为 2 和 $2^{127.48}$。这是首个对于全轮 GIFT-64 算法的安全性分析结果。

关键词：轻量级分组密码；GIFT 算法；密码分析；Biclique 分析；Star 攻击

中图分类号：TN918.1 doi: 10.19734/j.issn.1001-3695.2018.11.0826

Biclique analysis of GIFT-64

Guo Weibo[1], Liu Bin[1], Wang Yang[2]

(1. *Information Engineering University*, *Zhengzhou* 450001, *China*; 2. *Xi'an Division of Surveying & Mapping*, *Xi'an* 710054, *China*)

Abstract: GIFT is a lightweight block cipher with high efficiency and low power consumption. There are few research results to evaluate its security. This paper presented the balanced Biclique and Star attacks on GIFT-64 based on the Biclique attack method, combined with the information leakage of the key scheduling and the round function structure of GIFT-64. The data complexity and computational complexity required for the balanced Biclique attack of GIFT-64 are 2^{32} and $2^{127.36}$ respectively. The data complexity and computational complexity required for the Star attack of GIFT-64 are 2 and $2^{127.48}$ respectively. These are the first security analysis for the full-round GIFT-64.

Key words: lightweight block cipher; gift; cryptanalysis; Biclique analysis; star attack

0 引言

GIFT 算法是由 Banik 等人[1]于 CHES 2017 上提出的一种 SPN 结构的轻量级分组密码算法，适用于物联网、无线传感网络等资源受限的环境。该算法基于 PRESENT 算法[2]设计理念进行设计，但与 PRESENT 算法相比，所需的功耗更低，甚至具有更优的实现效率。GIFT 算法的密钥规模为 128 bit，根据分组规模的不同，可分为 GIFT-64 和 GIFT-128 这两种。

Biclique 分析方法由 Bogdanov 等人[3]于 2011 年 Asiacrypt 上提出的一种针对分组密码和哈希函数的新型攻击方法，其本质是基于中间相遇思想，利用差分攻击技术并借助密码算法结构和密钥调度的信息泄露规律实现密钥恢复的一种攻击方法。利用此攻击方法，一般能够实现对于全轮分组密码算法的安全性分析。最初被应用于对全轮 AES 算法[4]的攻击，且攻击复杂度低于穷举攻击，后续的，有一系列运用 Biclique 攻击方法分析其他分组密码算法安全性的分析结果，例如对 LBlock[5]、PRESENT[6]、Piccolo[7,8]等算法的安全性分析。

现有的对于 GIFT 算法的安全性分析结果较少，而由于 GIFT 算法采用与 PRESENT 算法类似的算法构造，因此对于 PRESENT 算法的一系列安全性分析方法对 GIFT 算法同样适用。其中，设计者在设计文档中简要分析了 GIFT 算法在差分分析、线性分析、不变子空间攻击、代数攻击等攻击方法下的安全性；赵静远等人[9]结合自动搜索技术，找到了 GIFT-64 算法的 10 轮差分区分器，并基于此区分器给出了 16 轮和 17 轮 GIFT-64 算法的差分分析结果。本文中利用 Biclique 分析方法，首次评估了全轮 GIFT-64 算法在平衡 Biclique 攻击和 Star 攻击下的安全性。

1 基础知识

1.1 GIFT 算法简介

GIFT 算法采用 SPN 结构进行设计，其设计理念与 PRESENT 算法类似，是由设计者为纪念 PRESENT 算法问世十周年推出了一种新的轻量级分组密码算法。与 PRESENT 相比，GIFT 算法的 S 盒不再受分支数为 3 的限制，且在算法的实现效率方面更优。

GIFT 算法根据分组规模不同，分为 GIFT-64 和 GIFT-128 两种，加密轮数分别为 28 轮和 40 轮，所使用的密钥量均为 128 比特。本文中主要分析 GIFT-64 算法在 Biclique 攻击下的安全性，因此此处仅对 GIFT-64 算法的具体结构进行介绍。

GIFT-64 算法的一轮轮函数顺序执行如下三个运算：S 盒变换；比特置换；密钥加变换。下面详细介绍这三个运算的具体过程，GIFT-64 算法的轮函数结构示意图如图 1 所示。

a)S 盒变换。GIFT 算法的 S 盒变换是算法唯一的非线性环节，其由 16 个相同的 4-bit 可逆 S 盒并置而成，对算法状态值的每一半子节均进行作用，达到混乱的效果。GIFT-64 算法所采用的 4-bit S 盒的具体结构如表 1 所示。

收稿日期：2018-11-10；**修回日期**：2019-01-16

作者简介：郭伟博（1980-），男，陕西周至人，讲师，硕士，主要研究方向为网络信息防御、算法分析（sjl1032011026@163.com）；刘彬（1984-），男，山东寿光人，讲师，硕士，主要研究方向为网络信息防御；王洋（1991-），男，陕西西安人，助理工程师，硕士，主要研究方向为信息安全、大数据．

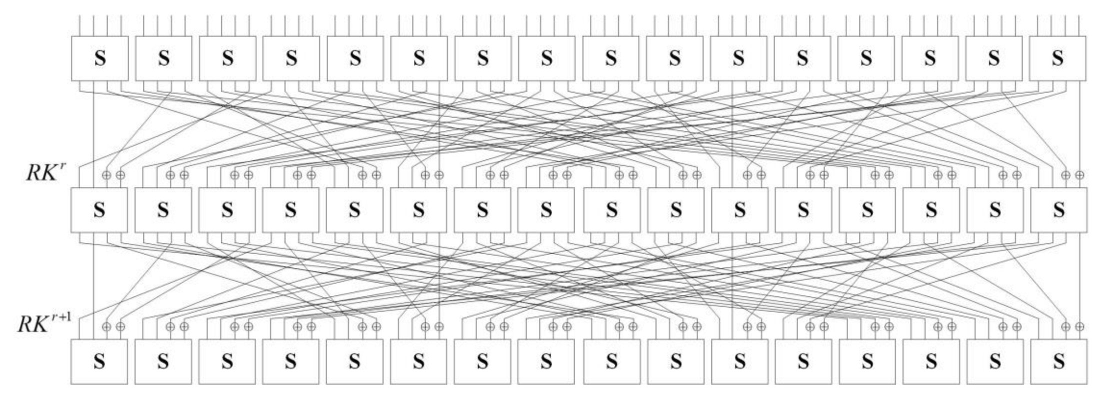


图 1 GIFT-64 算法轮函数

Fig. 1 Round function of GIFT-64

表 1 GIFT-64 算法的 4-bit S 盒

Table 1 The 4-bit S-box of GIFT-64

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
S(x)	1	a	4	c	6	f	3	9	2	d	b	7	5	0	8	e

b)比特置换。GIFT-64 算法的置换层是基于比特进行运算，实现将第 i 个比特位置的状态值置换为第 $P(i)$位，即

$$b_{P(i)} = b_i, \forall i \in \{0,1,...,63\}\ ,$$

该算法每一轮的输入状态从右至左依次为第 0 至第 63 个比特，表 2 给出了 GIFT-64 算法具体的置换表。

表 2 GIFT-64 算法的比特置换

Table 64 Bit permuation of GIFT-64

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P_{64}(i)$	0	17	34	51	48	1	18	35	32	49	2	19	16	33	50	3
i	16	17	18	19	20	21	22	36	24	25	26	27	28	29	30	31
$P_{64}(i)$	4	21	38	55	52	5	22	39	36	53	6	23	20	37	54	7
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P_{64}(i)$	8	25	42	59	56	9	26	43	40	57	10	27	24	41	58	11
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P_{64}(i)$	12	29	46	63	60	13	30	47	44	61	14	31	28	45	62	15

c)密钥加变换。该步骤由轮密钥加和轮常数加两部分组成。对于密钥加部分，通过密钥调度算法生成 32 bits 的轮密钥 RK^r， $r \in \{1,2,...,28\}$，将轮密钥划分成两部分，即

$$RK^r = U \| V = u_{15}...u_0 \| v_{15}...v_0\ ,$$

将 U 和 V 分别与状态值 $\{b_{4i+1}\}$ 和 $\{b_{4i}\}$ 异或得到

$$b_{4i+1} \leftarrow b_{4i+1} \oplus u_i\ ,\ b_{4i} \leftarrow b_{4i} \oplus v_i\ ,\ \forall i \in \{0,...,15\}$$

对于常数加部分，将单比特“1”和一个 6 比特常数 $C=c_5c_4c_3c_2c_1c_0$ 分别与状态值的第 63,23,19,15,11,7 和第 3 个比特进行异或，即

$$b_{63} \leftarrow b_{63} \oplus 1\ ,$$

$$b_{23} \leftarrow b_{23} \oplus c_5, b_{19} \leftarrow b_{19} \oplus c_4, b_{15} \leftarrow b_{15} \oplus c_3\ ,$$

$$b_{11} \leftarrow b_{11} \oplus c_2, b_7 \leftarrow b_7 \oplus c_1, b_3 \leftarrow b_3 \oplus c_0$$

密钥调度算法 对于 GIFT-64 算法，轮密钥 $RK^r = U \| V$ 由从密钥状态 $(k_7 \| k_6 \| ... \| k_0)$ 中提取的两个 16 比特字组成，且轮密钥的提取在密钥状态更新之前，即

$$U \leftarrow k_1, V \leftarrow k_0$$

密钥状态的更新方式如下：

$$k_7 \| k_6 \| ... \| k_0 \leftarrow k_1 >>> 2 \| k_0 >>> 12 \| ... \| k_3 \| k_2\ ,$$

这里的 $>>> j$ 表示在一个 16 比特字中循环右移 j 位。

轮常数定义为 $(c_5,c_4,c_3,c_2,c_1,c_0)$，其通过一个 LFSR 作用进行状态值更新，初始值置 0，采用如下函数进行状态更新：

$$(c_5,c_4,c_3,c_2,c_1,c_0) \leftarrow (c_4,c_3,c_2,c_1,c_0,c_5 \oplus c_4 \oplus 1)$$

表 3 给出了 GIFT-64 算法中各轮使用的轮常数。关于算法更多的设计细节详见文献[1]。

表 3 GIFT-64 算法的各轮轮常数

Table 3 Round constants of GIFT-64

轮数	轮常数													
1-14	01	03	07	0F	1F	3E	3D	3B	37	2F	1E	3C	39	33
15-28	27	0E	1D	3A	35	2B	16	2C	18	30	21	02	05	0B

1.2 Biclique 分析方法基本原理

Biclique 攻击首先需要构造 Biclique 结构，而 Bogdanov 等人在文献[3]给出的对于 AES 算法的平衡 Biclique 攻击中，提出了两种构造 Biclique 结构的方法，分别为 Independent Biclique 结构和 Long Biclique 结构。由于 Independent Biclique 结构的构造更为简易，且攻击轮数更长，所以后续的研究结果中一般采用此结构对密码算法进行 Biclique 分析，本文中同样如此。而在进行具体攻击时，根据构造所得结构维数不同，还可分为平衡 Biclique 攻击、非平衡 Biclique 攻击和 Star 攻击。下面介绍 Biclique 结构和 Biclique 攻击具体步骤。

1)Biclique 结构

一般来讲，一个 Biclique 结构就是一个二分图，通常用三元组的形式进行表示。令 r 轮子算法 f 在密钥 $K[i, j]$ 作用下将密文状态 C 中的 2^{d_1} 个元素 C^i 映射到中间状态 S 中的 2^{d_2} 个元素 S^j，也就是 $S^j \xleftarrow[f]{K[i,j]} C^i$ ， $\forall i \in \{0,1,...,2^{d_1-1}\}, \forall j \in \{0,1,...,2^{d_2-1}\}$ 。

将这样的三元组 $(\{C^i\},\{S^j\},K[i,j])$ 记为 (d_1,d_2) 维 Biclique 结构。若 $d_1 = d_2 = d \neq 0$，则称为平衡 Biclique 结构，若 $d_1 = 0, d_2 = d' \neq 0$，则称为 Star 结构， $d_1 \neq d_2$ 且均不为 0 时为非平衡 Biclique 结构。图 2 表示一般的密文方向的 Biclique 结构，相应的，根据算法实际，还可以构造明文方向的 Biclique 结构用于实施攻击。

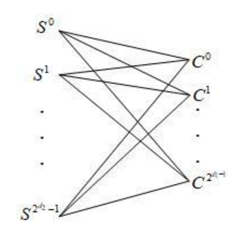


图 2 Biclique 结构

Fig. 2 Biclique structure

2)Biclique 攻击流程

将一个分组密码 E_K 看做多个子算法的结合，即使得由密文状态 C 映射到明文状态 P 有如下表示：

$$P \xleftarrow{e_2} V \xleftarrow{e_1} S \xleftarrow{f} C$$

其中 f 表示构造 Biclique 结构的子算法，e_1 和 e_2 分别表示匹配阶段的子算法，V 表示匹配向量，进而可将 Biclique 攻击分为以下四步：密钥划分；构造 Biclique 结构；状态匹配；

密钥筛选。

攻击所需的复杂度主要包括数据复杂度和计算复杂度。其中，数据复杂度由进行 Biclique 结构构造时所需的选择明（密）文数量决定，计算复杂度主要三部分组成，即 Biclique 结构构造、状态匹配以及密钥筛选所需的计算复杂度。由于 GIFT-64 算法的非线性部件 S 盒占用的计算资源明显多于其他环节，因此在本文中进行计算复杂度估计时，近似的以所需计算的 S 盒个数来估计攻击所需的计算复杂度。且为了进一步降低攻击所需的计算复杂度，在上述介绍的状态匹配过程中，攻击者通过检验前向和后向匹配过程得到的匹配向量值是否一致，筛选错误密钥，此时，还可以利用预计算匹配技术[3]降低匹配阶段的计算复杂度。

2　GIFT-64 算法的平衡 Biclique 分析

首先，本文利用文献[3]中构造 Biclique 结构的方法，通过合适的密钥划分，构造得到了一个明文方向的 5 轮(4,4)平衡 Biclique 结构。进一步地，给出了全轮 GIFT-64 算法的安全性分析结果。

a)密钥划分。根据密钥调度算法，选取 $k_2[0,12],k_3[0,4],k_4[0,1],k_5[0,1]$ 为活动比特位。令 $K[0,0]$ 为上述 8 比特位置密钥为 0，其余位置遍历的主密钥。将 128 比特主密钥划分为 2^{120} 个集合，每一密钥集合中包含 2^8 个密钥 $K[i,j]$。这里的 $K[i,j]$ 由 $K[0,0]$ 与密钥差分 Δ_i^k 和 ∇_j^k 组成，其中 $\Delta_i^k=(k_2[0,12],k_3[0,4])$，$\nabla_j^k=(k_4[0,1],k_5[0,1])$。

b)构造平衡 Biclique 结构。基于上述划分的密钥空间，通过相应的轮密钥构造对应的相关密钥差分特征 Δ_i 和 ∇_j，经分析可得，(Δ_i,∇_j) 中无重合的 S 盒，即两者相互独立，也就是说构造得到了一个 5 轮 (4,4) 平衡 Biclique 结构 $(\{P^i\},\{S^j\},K[i,j])$。图 3 给出了具体结构。

c)状态匹配。根据构造得到的 5 轮(4,4)平衡 Biclique 结构，得到 2^4 个明文状态 P^i，通过正确密钥解密得到对应的 2^4 个密文状态 C^i，选择第 17 轮的第 44-47 个输出比特为匹配向量。由 C^i 向上解密 11 轮，称为后向匹配阶段，S^j 向下加密 12 轮，称为前向匹配阶段，图 4 给出了平衡 Biclique 攻击的状态匹配过程，由图可得，在前向匹配阶段只需对图中 32 个 S 盒进行预计算，12 个 S 盒进行 2 次重计算，4 个 S 盒进行 2^2 次重计算，148 个 S 盒进行 2^4 重计算；在后向匹配阶段，只需对图中 36 个 S 盒进行预计算，4 个 S 盒进行 2 次重计算，8 个 S 盒进行 2^2 次重计算，101 个 S 盒进行 2^4 重计算，即可完成匹配。图 4 中白色表示不需计算的 S 盒，淡灰色表示需预计算的 S 盒，灰色表示需重计算的 S 盒。

综上，对于 GIFT-64 算法的(4,4)平衡 Biclique 攻击所需的数据复杂度为 2^{32} 个选择明文，计算复杂度为 $2^{127.36}$ 次全轮 GIFT-64 加密。证毕。

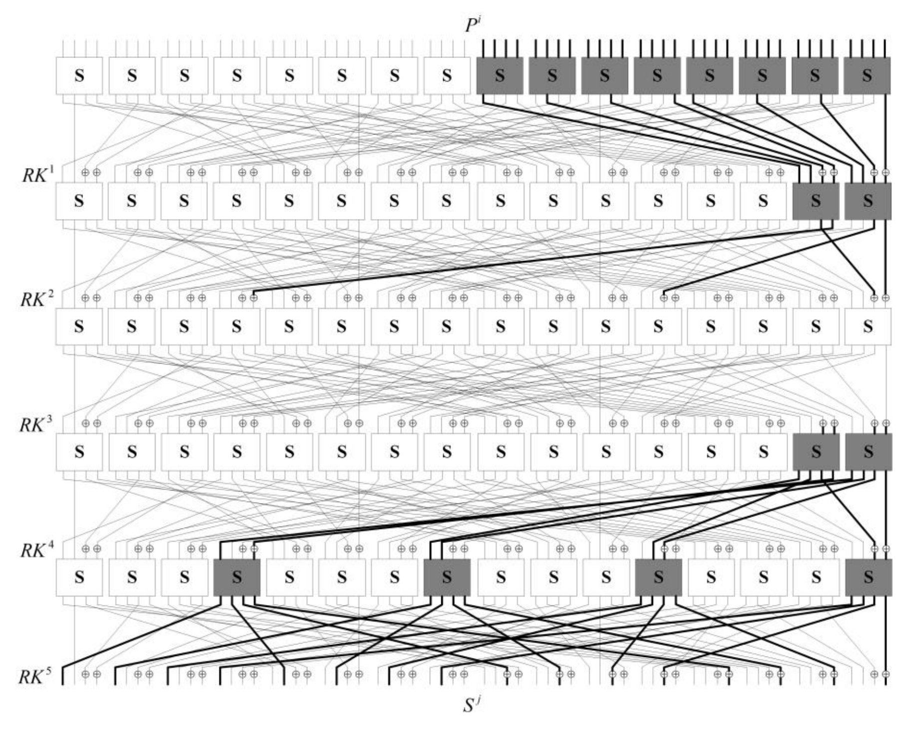


图 3　5 轮（4,4）平衡 Biclique 结构

Fig. 3　5-round (4,4) Balanced Biclique structure

d)密钥筛选。由于使用的匹配向量为第 44~47 bit 共 2^4 个可能值，即得平均一个错误密钥通过筛选的概率为 2^{-4}。又根据每个密钥集合中含有 2^8 个密钥，所以每个密钥集合平均有 $2^8\times2^{-4}=2^4$ 个密钥通过筛选，即得到了 2^4 个候选密钥。最后，对每个集合中剩余的 2^4 个候选密钥进行全轮加密，检验得到初始的正确密钥。上述 GIFT-64 算法平衡 Biclique 攻击所需的复杂度指标由定理 1 给出。

定理 1　采用 5 轮(4,4)平衡 Biclique 结构对 GIFT-64 算法进行安全性分析，可恢复全轮 GIFT-64 算法的主密钥，攻击所需的数据复杂度为 2^{32}，计算复杂度为 $2^{127.36}$。

证明　攻击所需数据复杂度主要为构造平衡 Biclique 结构所需的选择明文量，根据图 3 可得，对于每一个 Biclique 结构，需遍历明文的第 0-31 个比特，第 32-63 个比特固定，即得数据复杂度为 2^{32} 个选择明文。

攻击所需的计算复杂度主要包含三部分。一是构造 Biclique 结构，由图 3 可得，构造过程需对 64 个 S 盒进行预计算，12 个 S 盒进行 2^2 次重计算，4 个 S 盒进行 2^4 重计算，即结构构造过程中共需计算 176 个 S 盒。二是状态匹配，主要包含前向匹配和后向匹配两个阶段。根据上述攻击过程可得，前向匹配阶段预计算 32 个 S 盒，对 12 个 S 盒进行 2 次重计算，4 个 S 盒进行 2^2 次重计算，148 个 S 盒进行 2^4 重计算，即需计算 $2^4\times(32+2\times12+2^2\times4+2^4\times148)=39040$ 个 S 盒；后

向匹配需要预计算 36 个 S 盒，对 4 个 S 盒进行 2 次重计算，8 个 S 盒进行 2^2 次重计算，101 个 S 盒进行 2^4 重计算，即需计算 $2^4\times(36+2\times4+2^2\times8+2^4\times101)=27072$ 个 S 盒。也就是说，匹配阶段所需计算的 S 盒个数总计为：$39040+27072=66112$。三是密钥筛选，由每一密钥子集合剩余 2^4 候选密钥，则 $C_{flase}=2^4$。因此上述攻击所需的计算复杂度总计为 $C=2^{120}\times(\frac{176+66112}{28\times16}+2^4)\approx 2^{127.36}$ 次全轮 GIFT-64 加密。

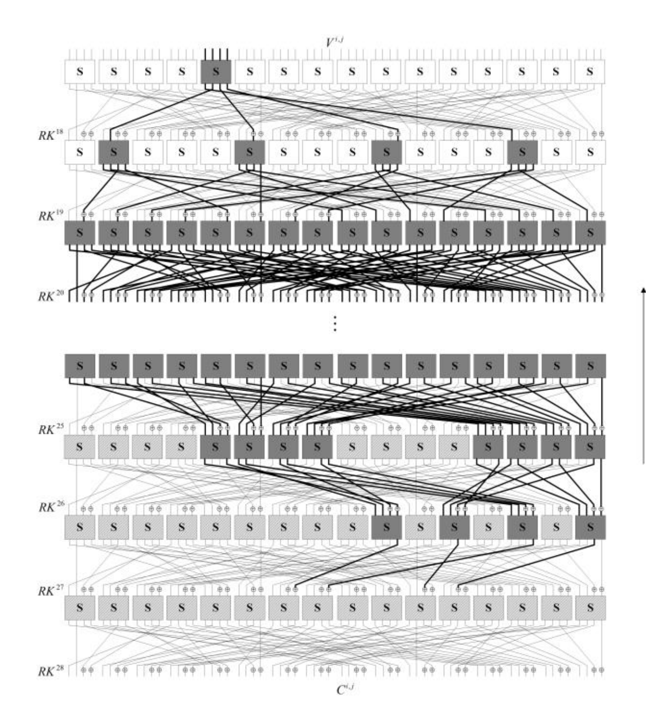


图 4　GIFT-64 算法平衡 Biclique 攻击的状态匹配过程

Fig. 4　Matching phase of balanced Biclique attack on GIFT-64

3　GIFT-64 算法的 Star 攻击

上一章中主要运用平衡 Biclique 攻击方法分析了全轮 GIFT-64 算法的安全性,在本节中主要考虑运用 Star 攻击给出对于全轮 GIFT-64 最低数据复杂度的攻击结果。Star 攻击最先是由 Bogdanov 等人[11]于 2014 年提出的一种非平衡 Biclique 攻击方法,最早应用于分析 AES 算法的安全性。该攻击方法的攻击过程与平衡 Biclique 攻击过程基本一致,但所需数据复杂度很少,一般为 2~3 个已知明文,相应的计算复杂度就有所增加,下面给出针对 GIFT-64 算法 Star 攻击的具体步骤。

a) 密钥划分。基于密钥调度算法，选取 $k_4[0,1,8,11],k_5[0,1,8,11]$ 为活动比特位。令 $K[0,0]$ 为上述 8 比特位置密钥为 0，其余位置遍历的主密钥。将 128 比特主密钥划分为 2^{120} 个集合，每一密钥集合中包含 2^8 个密钥 $K[i,j]$。这里的 $K[i,j]$ 由 $K[0,0]$ 与密钥差分 Δ_i^k 和 ∇_j^k 组成，其中 $\Delta_i^k=(k_4[0,1],k_5[0,1])$，$\nabla_j^k=(k_4[8,11],k_5[8,11])$。

b)构造 Star 结构。基于上述划分的密钥空间，通过相应的轮密钥构造对应的相关密钥差分特征 Δ_i 和 ∇_j，与平衡 Biclique 结构一样，(Δ_i,∇_j) 中无重合的 S 盒，即两者相互独立，也就是说构造得到了一个 4 轮 8 维 Star 结构。图 5 给出了具体结构。

c)状态匹配。根据构造得到的 4 轮 8 维 Star 结构，与上一节的攻击过程类似，选择第 16 轮的第 44-47 个输出比特为匹配向量。在前向匹配阶段只需对 8 个 S 盒进行预计算，8 个 S 盒进行 2^4 重计算，164 个 S 盒进行 2^8 重计算；在后向匹配阶段，只需 34 个 S 盒进行预计算，4 个 S 盒进行 2 次重计算，2 个 S 盒进行 2^2 次重计算，8 个 S 盒进行 2^4 重计算，117 个 S 盒进行 2^8 重计算，即可完成匹配。图 6 给出了状态匹配阶段的具体路径，图中所用的颜色标志与图 4 相同。

d)密钥筛选。由于使用的匹配向量为 16 轮输出状态的第 44-47 个比特共 2^4 个可能值，即得平均一个错误密钥通过筛选的概率为 2^{-4}。又根据每个密钥集合中含有 2^8 个密钥，所以每个密钥集合平均有 $2^8\times2^{-4}=2^4$ 个密钥通过筛选，即得到了 2^4 个候选密钥。最后，对每个集合中剩余的 2^4 个候选密钥进行全轮加密，验证得到正确密钥。上述 GIFT-64 算法 Star 攻击所需的复杂度指标由定理 2 给出。

定理 2　采用 4 轮 8 维 Star 结构对 GIFT-64 算法进行安全性分析，可恢复全轮 GIFT-64 算法的主密钥，攻击所需的数据复杂度为 2，计算复杂度为 $2^{127.48}$。

证明　攻击所需的计算复杂度同样包含三部分。一是构造 Star 结构，由图 5 可得，构造过程需对 60 个 S 盒进行预计算，4 个 S 盒进行 2^2 次重计算，即结构构造过程中共需计算 76 个 S 盒。二是状态匹配，主要包含前向匹配和后向匹配两个阶段。根据上述攻击过程可得，在前向匹配阶段只需对 8 个 S 盒进行预计算，8 个 S 盒进行 2^4 重计算，164 个 S 盒进行 2^8 重计算，即需计算 42120 个 S 盒；在后向匹配阶段，只需 34 个 S 盒进行预计算，4 个 S 盒进行 2 次重计算，2 个 S 盒进行 2^2 次重计算，8 个 S 盒进行 2^4 重计算，117 个 S 盒进行 2^8 重计算。即需计算 30130 个 S 盒。也就是说，匹配阶段所需计算的 S 盒个数总计为：$42120+30130=72250$。三是密钥筛选，由每一密钥子集合剩余 2^4 候选密钥，则 $C_{flase}=2^4$。因此上述攻击所需的计算复杂度总计为 $C=2^{120}\times(\frac{76+72250}{28\times16}+2^4)\approx 2^{127.48}$ 次全轮 GIFT-64 加密。数据复杂度方面，使用 2 个明密文对，使得攻击成功率为 1。

综上，对于 GIFT-64 算法的 Star 攻击所需的数据复杂度为 2 个选择明文，计算复杂度为 $2^{127.48}$ 次全轮 GIFT-64 加密。证毕。

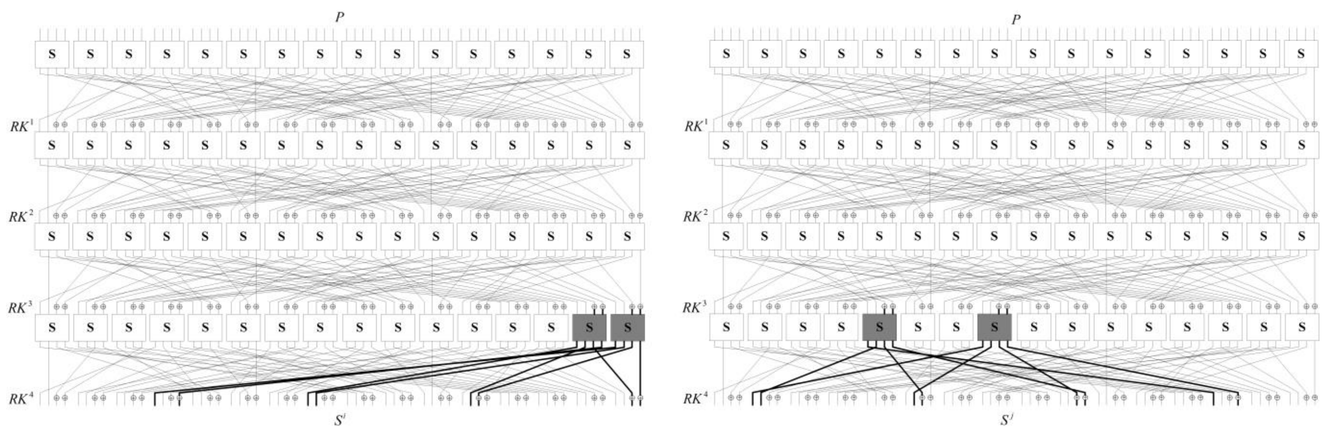
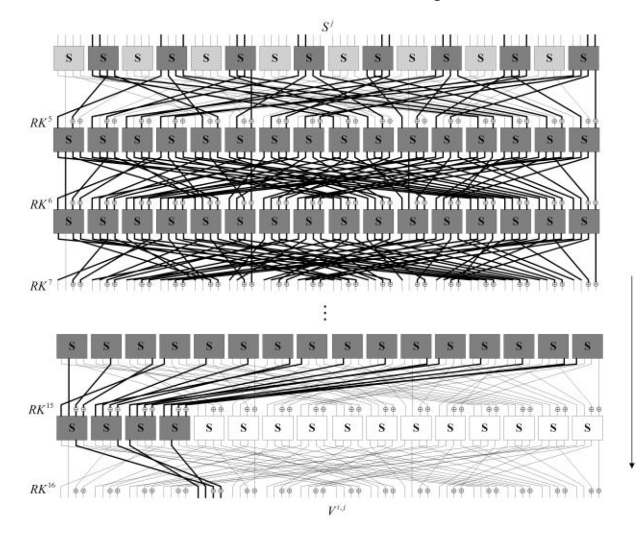


图 5　GIFT-64 算法 4 轮 8 维 Star 结构

Fig. 4　Rounds of 8-dimensional Star structure of GIFT-64



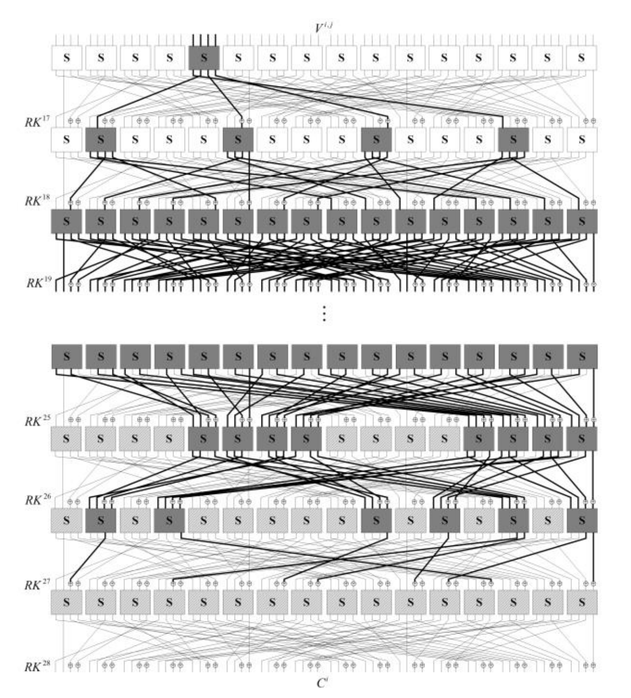


图 6　GIFT-64 算法 Star 攻击匹配阶段

Fig. 6　Matching phase of Star attack on GIFT-64

4　结束语

本文利用 Biclique 攻击方法分析了 GIFT-64 算法在平衡 Biclique 攻击和 Star 攻击下的安全性，结合 GIFT-64 算法线性密钥调度算法的信息泄露规律，分别给出了首个对于全轮 GIFT-64 算法最优计算复杂度和最低数据复杂度的安全性分析结果。下一步工作主要考虑利用 Biclique 攻击方法实现对于 GIFT-128 算法的安全性分析，扩充 GIFT 系列算法的安全性分析结果。

参考文献：

[1] Banik S, Pandey S K, Peyrin T, *et al.* GIFT: a small PRESENT [C]、、Proc of International Conference on Cryptographic Hardware and Embedded Systems. Cham：Springer, 2017: 321-345.

[2] Bogdanov A, Knudsen L R, Leander G, *et al.* PRESENT: an ultra-lightweight block cipher [C]//Proc of International Workshop on Cryptographic Hardware and Embedded Systems. Berlin:Springer, 2007: 450-466.

[3] Bogdanov A, Khovratovich D, Rechberger C. Biclique cryptanalysis of the full AES [C]//Advances in Cryptology. 2011: 344-371.

[4] National Institute of Standard and Technology (NIST). Federal information processing standards publication 197 (FIPS Pub 197): specification for the advanced encryption standard (AES)[S]. 2001.

[5] Wang Yanfeng, Wu Wenling, Yu Xiaoli, *et al.* Security on LBlock against biclique cryptanalysis[C]//Proc of International Workshop on Information Security Applications. Berlin:Springer, 2012: 1-14.

[6] Jeong K, Kang H C, Lee C, *et al.* Biclique cryptanalysis of lightweight block ciphers PRESENT, piccolo and LED [J]. IACR Cryptology ePrint Archive, 2012, 2012: 621.

[7] Wang Yanfeng, Wu Wenling, Yu Xiaoli, *et al.* Biclique Cryptanalysis of Reduced-Round Piccolo Block Cipher [C]//Proc of International Conference on Information Security Practice and Experience. Berlin:Springer, 2012: 337-352.

[8] Ahmadi S, Ahmadian Z, Mohajeri J, *et al.* Low-data complexity biclique cryptanalysis of block ciphers with application to Piccolo and Hight [J]. IEEE Trans on Information Forensics and Security, 2014, 9(10): 1641-1652.

[9] 赵静远，徐松艳，张子剑，等. 轻量级分组密码算法 GIFT 的差分分析[J].密码学报, 2018, 5(4): 335-343. (Zhao Jingyuan, Xu Songyan, Zhang Zijian, et al. Differential analysis of lightweight block cipher

GIFT[J]. Journal of Cryptologic Research, 2018, 5(4): 335-343.)
[10] Bogdanov, A. , Chang, D. , Ghosh, M. , *et al.* Biclique with minimal data and time complexity for AES [C]//Information Security and Cryptology.2014: 160-174.
[11] 崔竞一, 郭建胜, 刘翼鹏. 广义 Independent Biclique 攻击框架及其应用[J].计算机学报, 2018, 41(2):349-367. (Cui Jingyi, Guo Jiansheng, Liu Yipeng. Generalized Independent Biclique automated attack framework and its applications[J]. Chinese Journal of Computers, 2018, 41(2): 349-367.)